Lab 8b – Packets – Packet Analysis

By

Lukas Fuller

IAE-201-D02

IA-201: Introduction to Information Assurance

**Abstract**

The objective of this lab is to introduce students to Wireshark and packet analysis. The students will be able to use Wireshark to analyze packets on a network. Students will also be introduced to what network packets are.

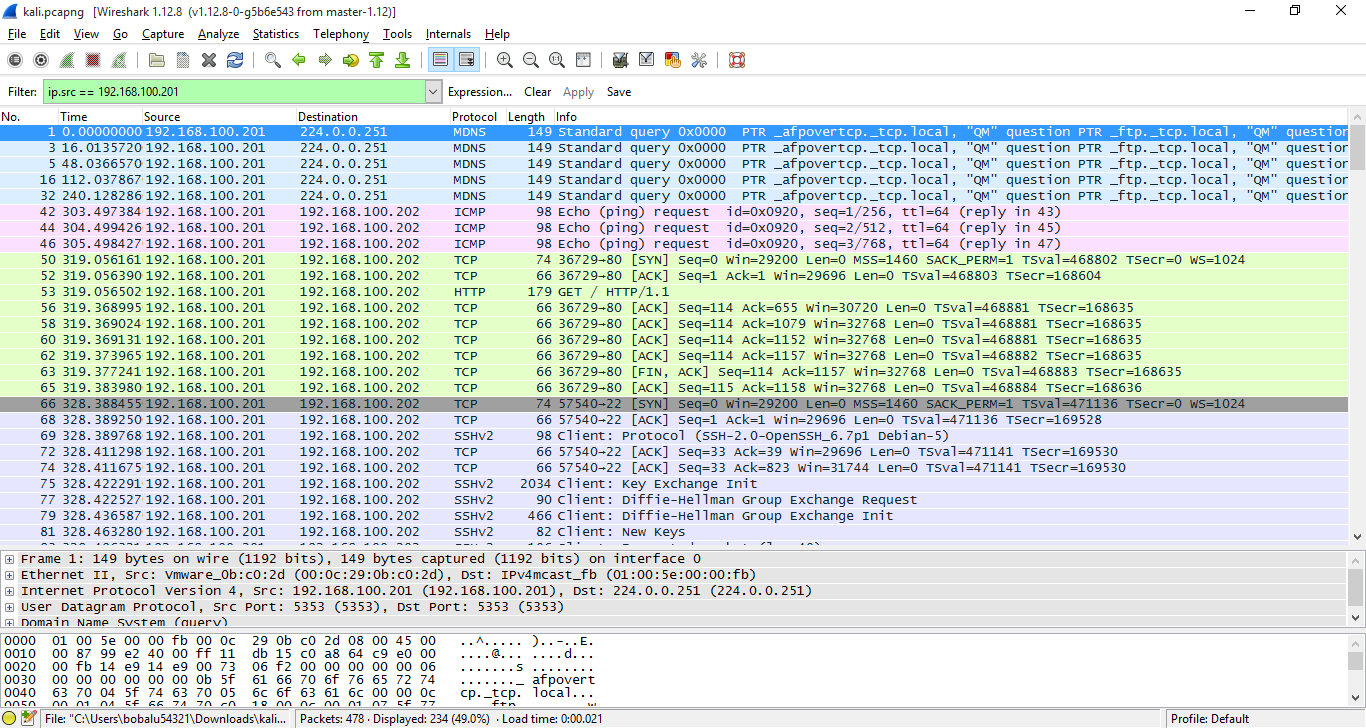
**Materials**

1. Kali Linux Virtual Machine
2. Metasploitable Virtual Machine

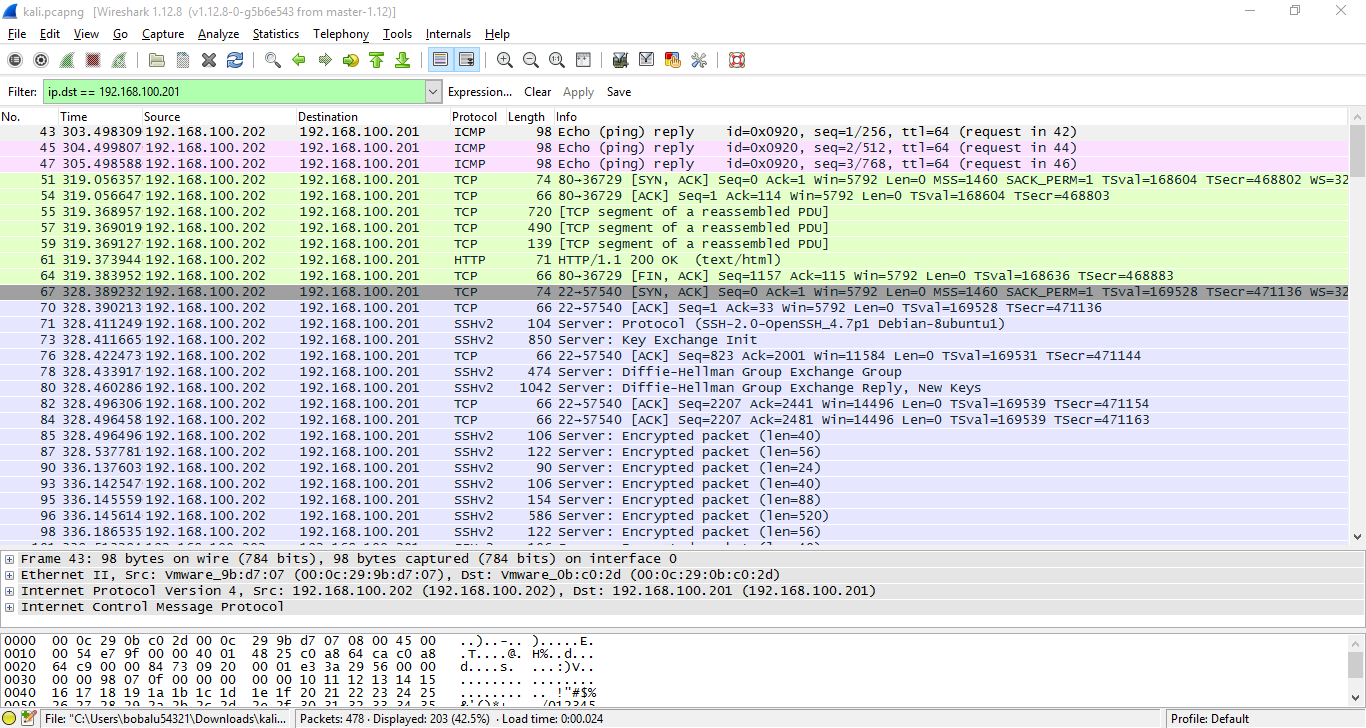
**Conclusion**

It was quite interesting to see how each packet is displayed, with several parameters that you are able to enlarge for greater specificity, and it was quite user friendly in general. Another important part I noticed was how encrypted data looks vs unencrypted, which of course is self-explanatory really, but seeing it for myself was still helpful. Lastly, being able to view the bits of data on each packet was helpful in understanding how they work. Overall, this lab helped me understand how to use wireshark and made the importance of using https even more clear.

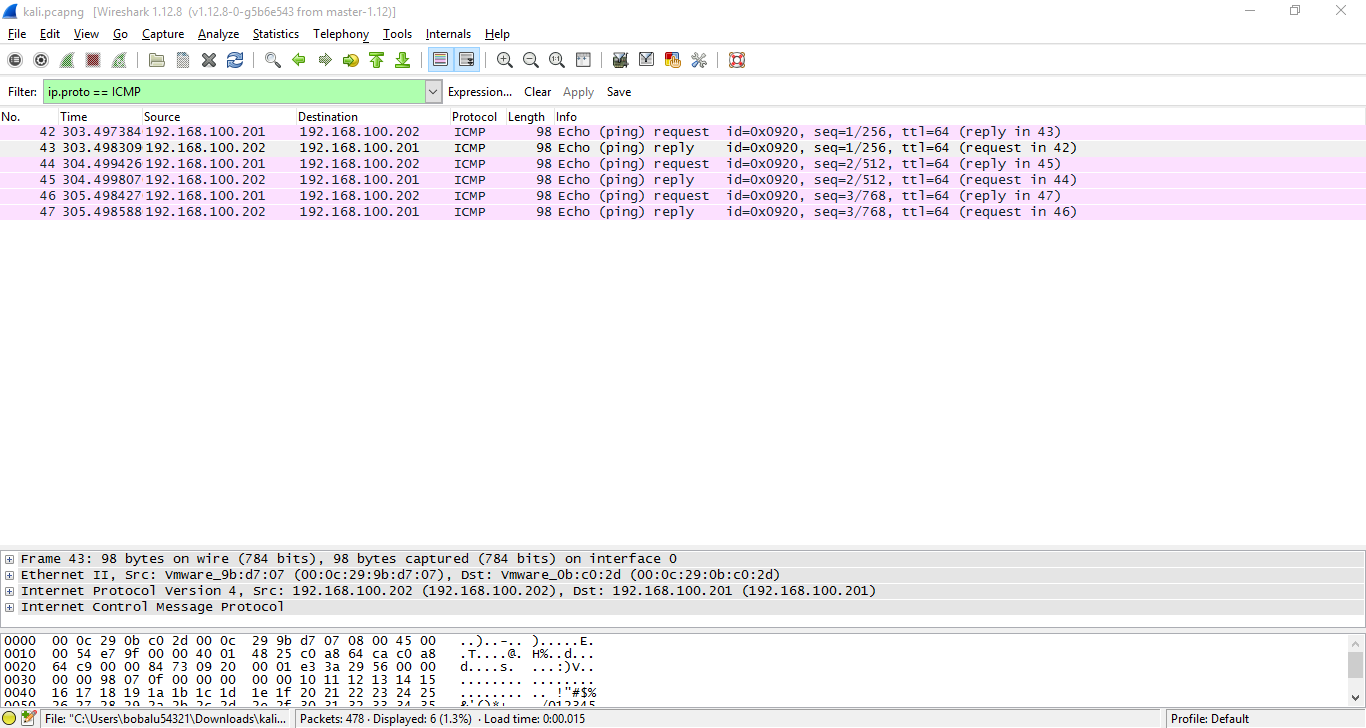
**Screenshots**

1. Screenshot of filtering packets sent from IP address 192.168.100.201.

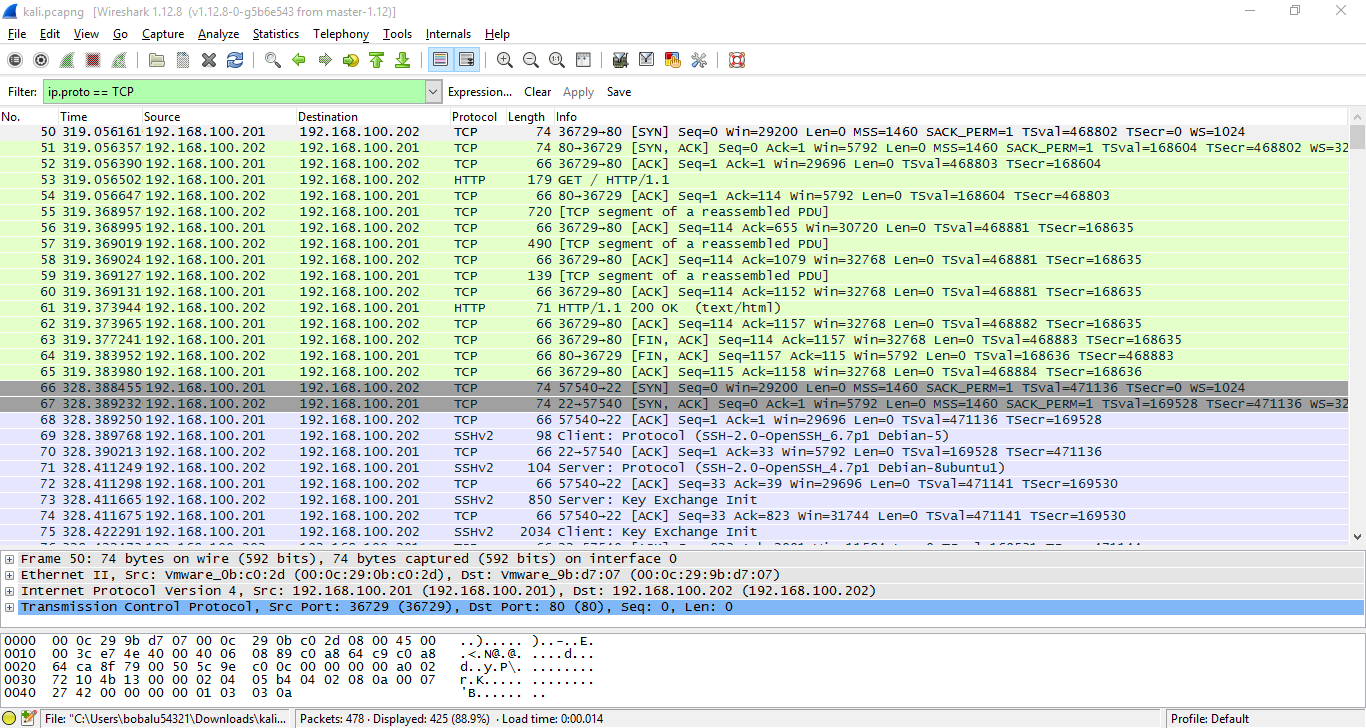
2. Screenshot of filtering packets sent to IP address 192.168.100.201.



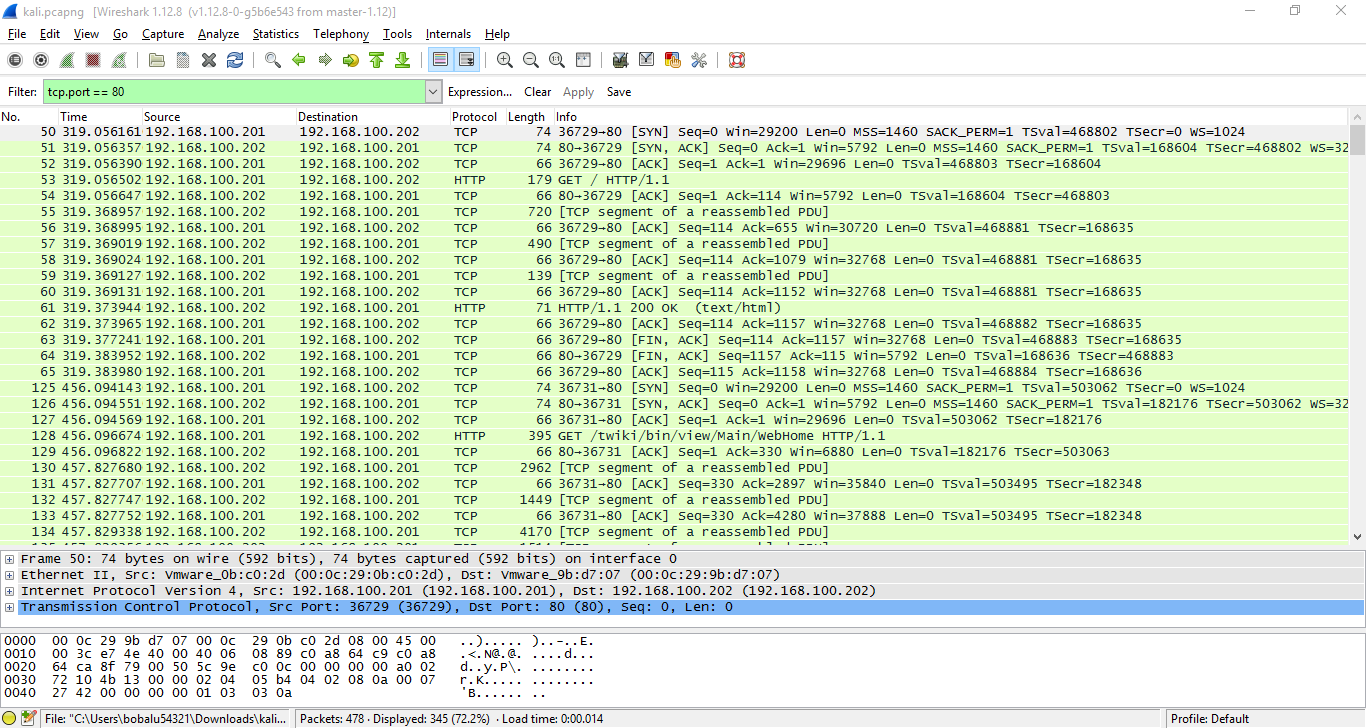
1. Screenshot of filtering packets sent via the ICMP protocol.



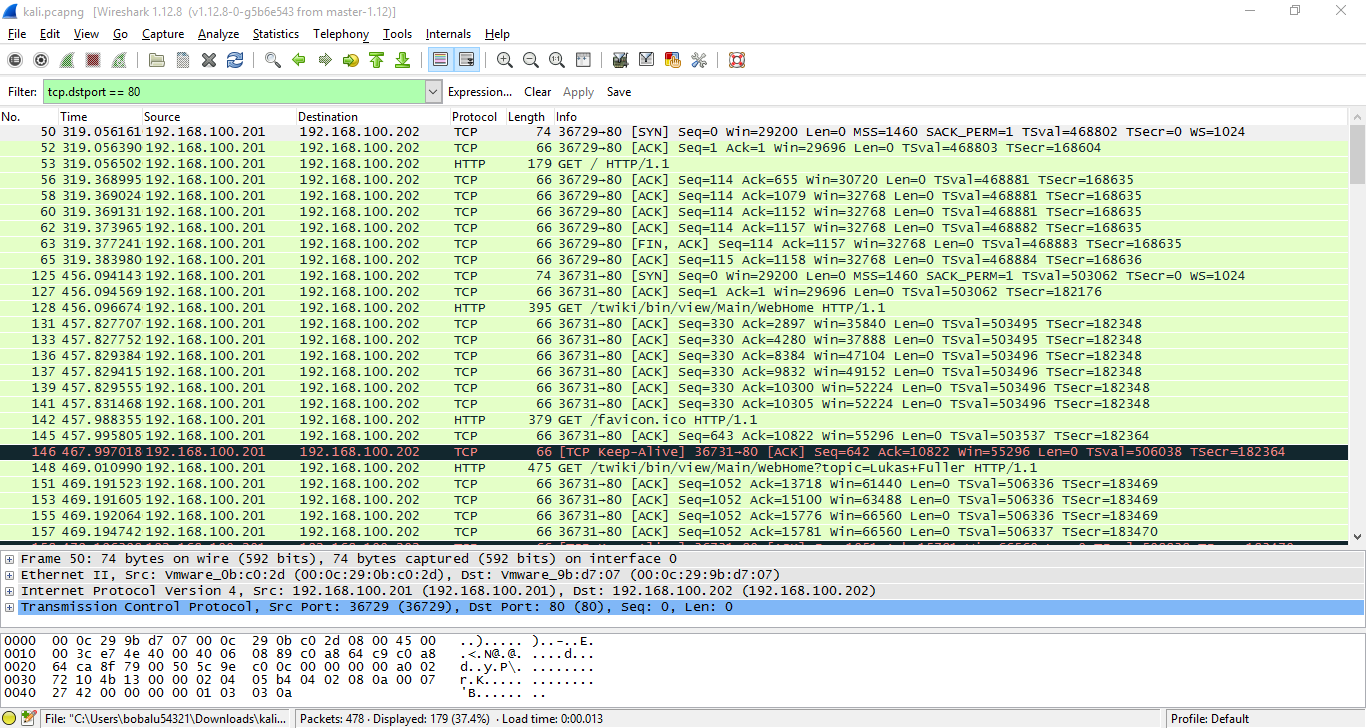
1. Screenshot of filtering packets sent via the TCP protocol.

****

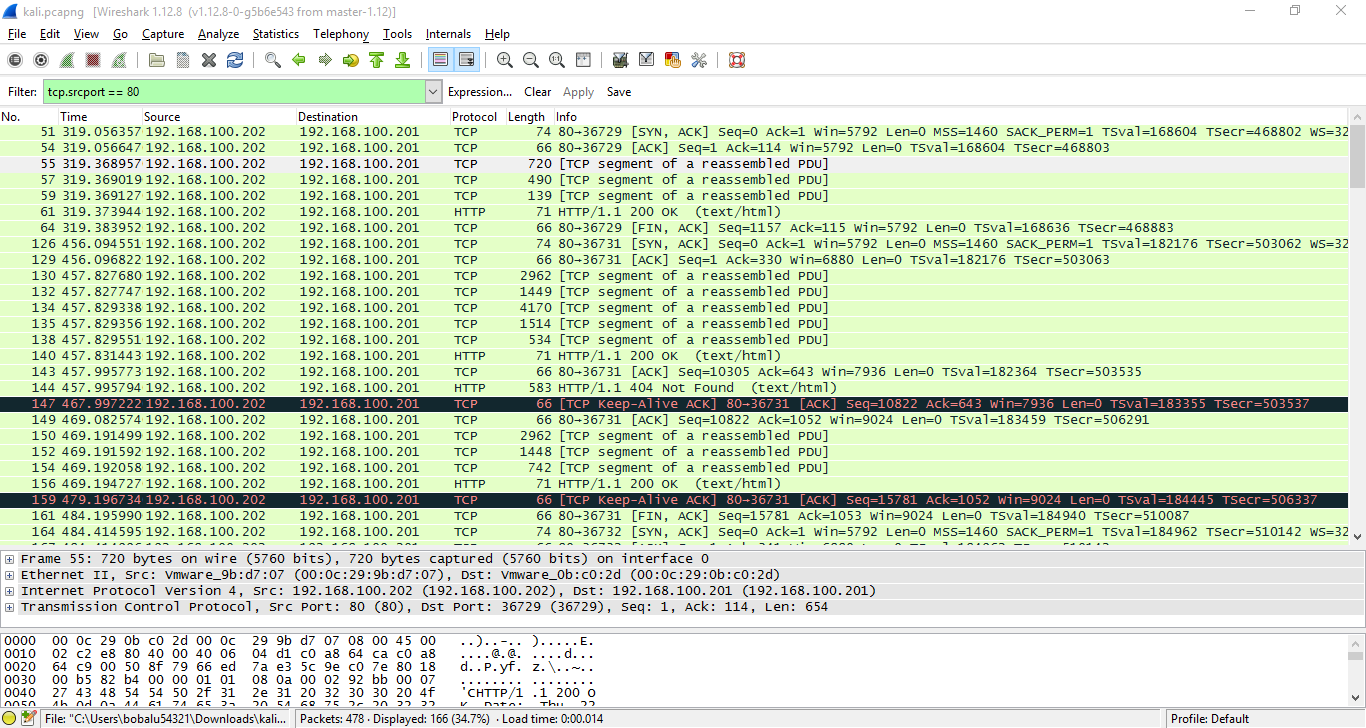
1. Screenshot of filtering packets sent via TCP port 80.



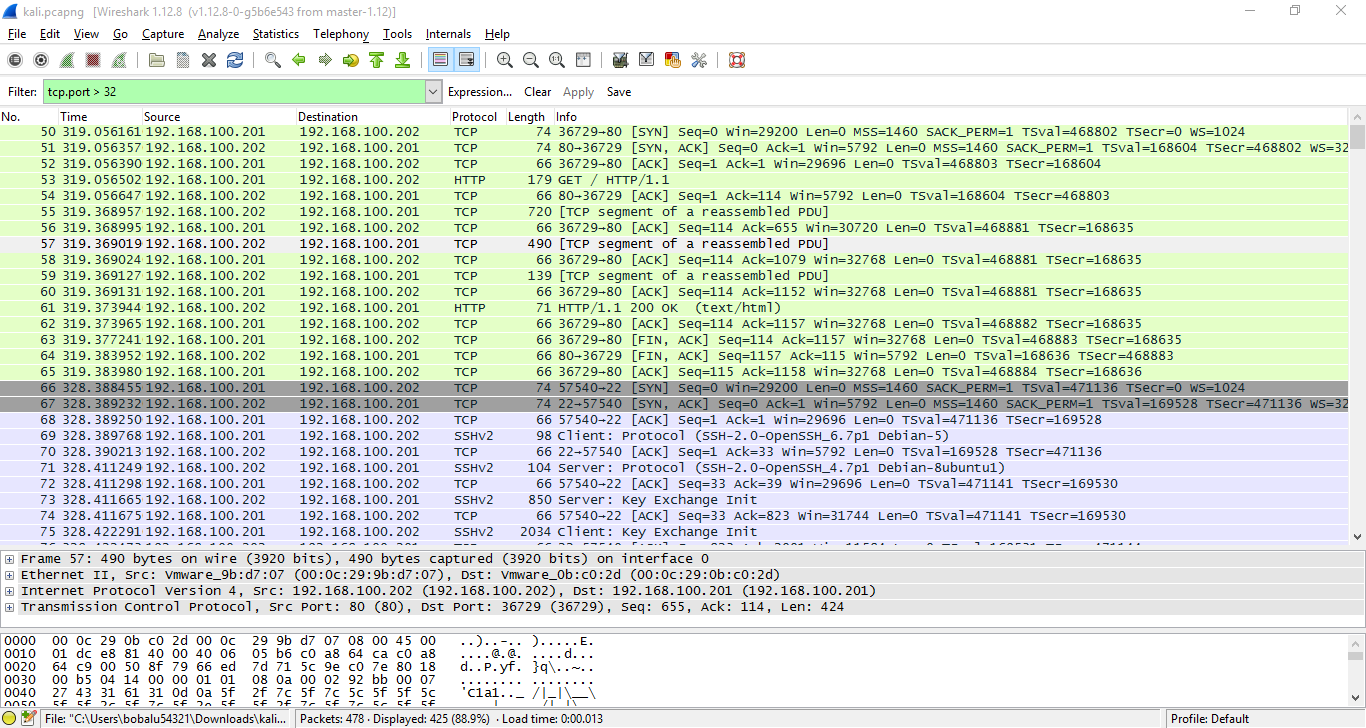
1. Screenshot of filtering packets sent via TCP port 80.

****

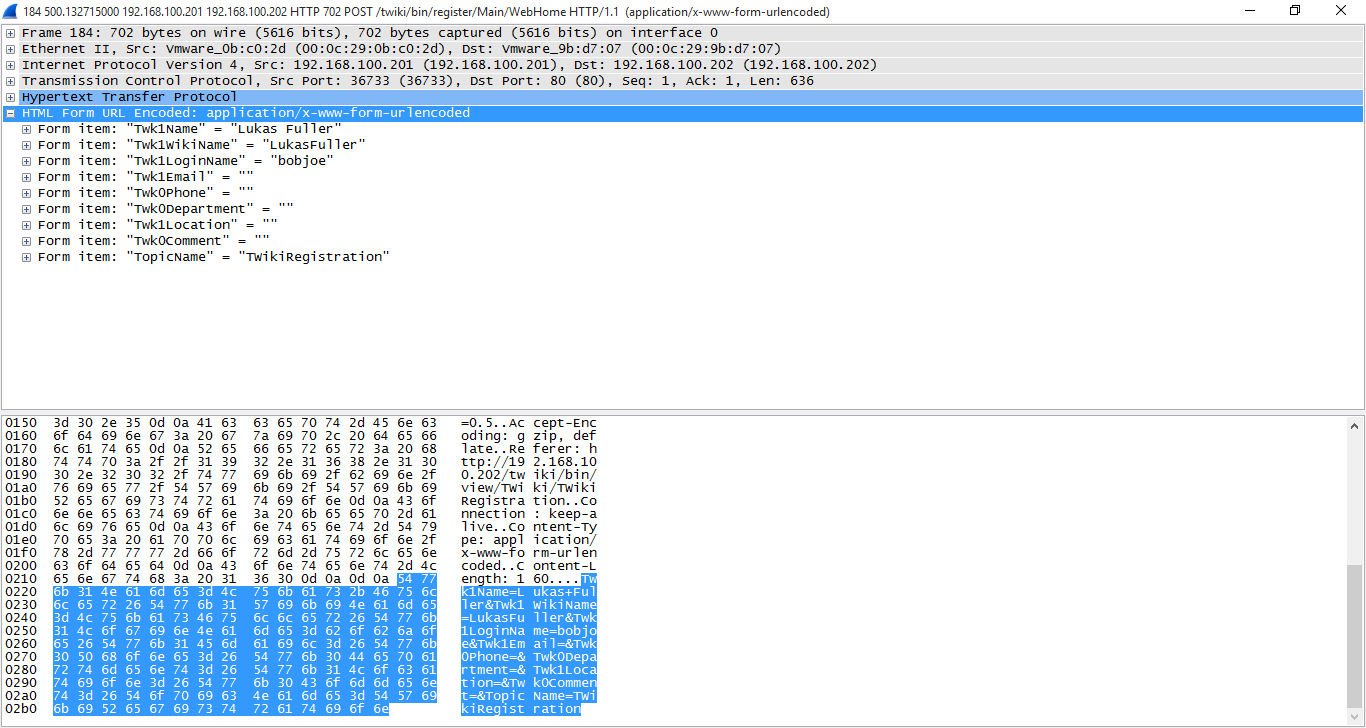
1. Screenshot of filtering packets sent from TCP port 80.



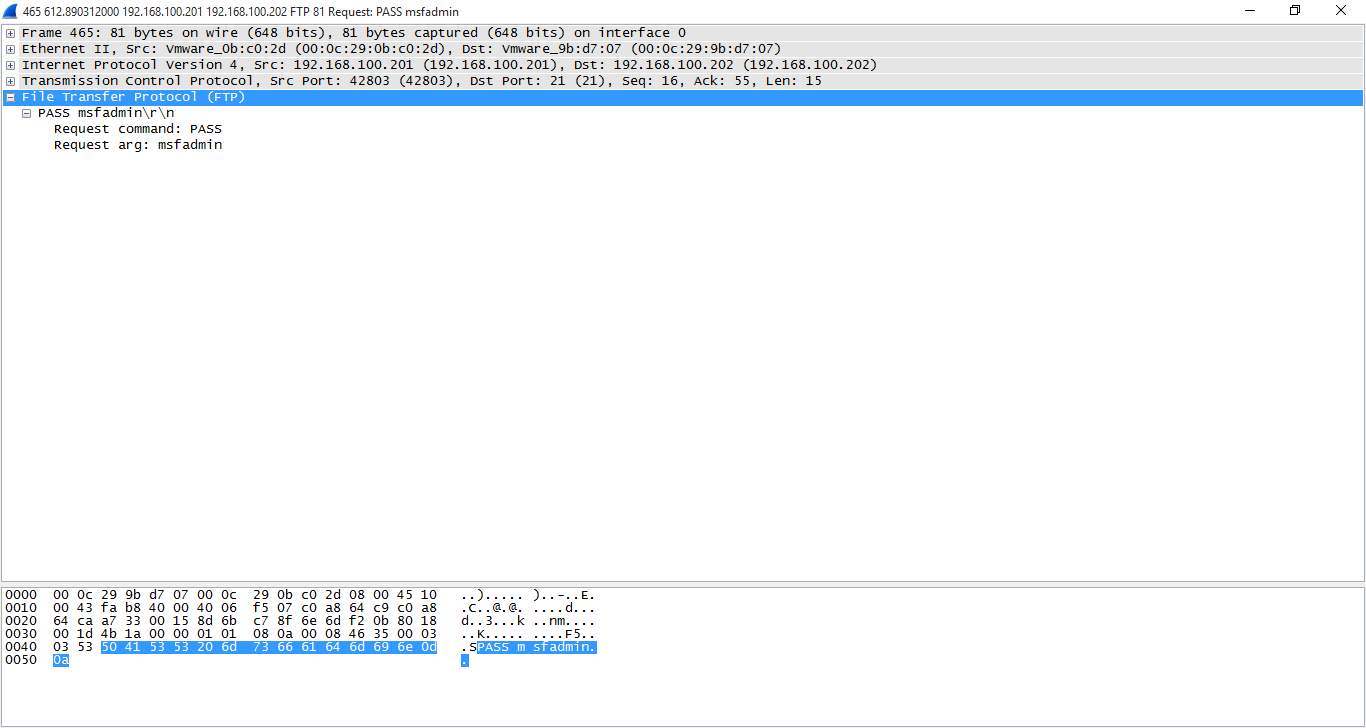
1. Screenshot of filtering packets sent via TCP ports greater than 32.



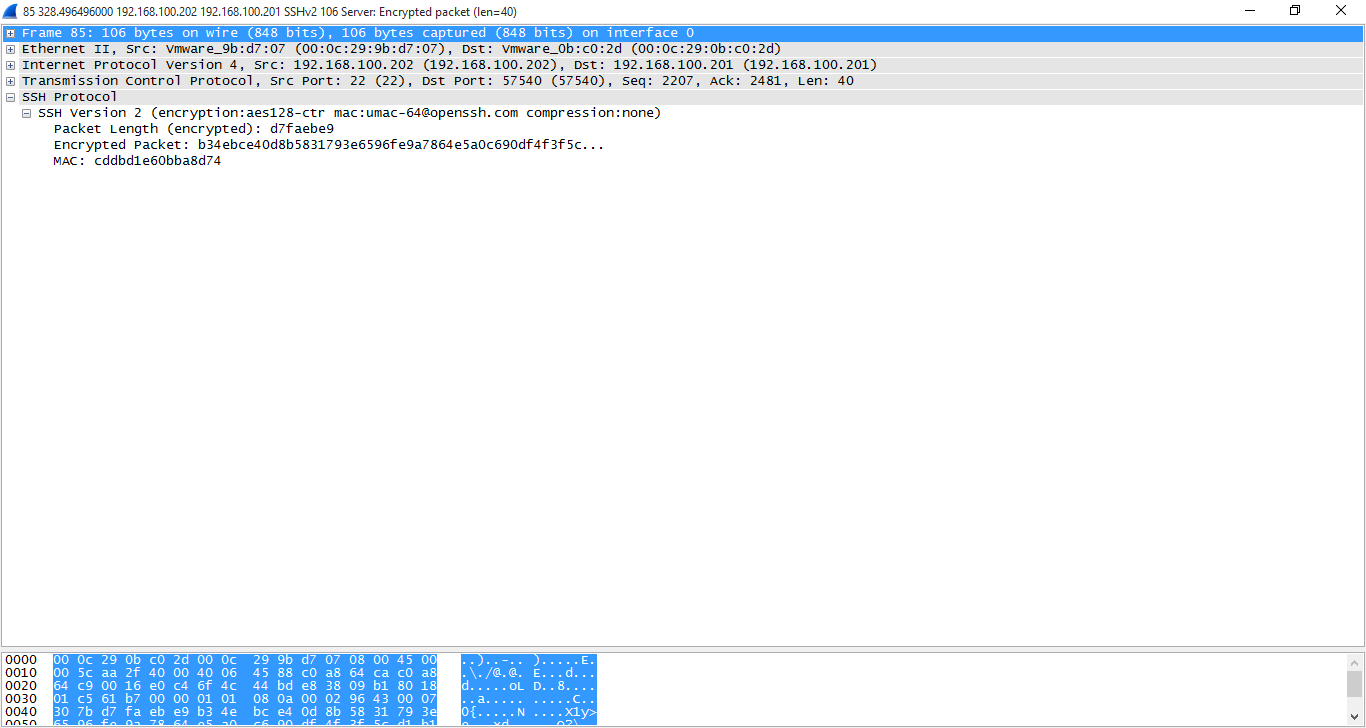
1. Screenshot of analyzing HTML form submission on HTTP server.



1. Screenshot of analyzing FTP password request.



1. Screenshot of analyzing SSH response.

****

**Questions:**

1. What is packet analysis? **Identifying what is inside each packet, and the seeing the conversation between the client to server**
2. What does filtering do in Wireshark? **It filters out the unwanted information through different search parameters (like searching for only TCP from a specific address)**
3. What is a dropped packet? **A packet that wasn’t successfully transmitted**
4. What is the expression to filter packets with the UDP port of 6432**? udp.dstport == 6432**
5. What is the expression to filter packets with a TCP port greater than 1024? **tcp.port > 1024**
6. Why is it important to use HTTPS and not HTTP (in reference to this lab)? **http is unencrypted and can easily be seen on wireshark, while https only displays the encrypted information so you can’t easily see private information on wireshark**
7. What is the encryption that SSH uses that you found in your analysis? **AES-128 encryption**
8. What is the version of HTTP that you found in your analysis? **1.1**
9. What FTP server did you find running in your analysis? **Version 4**
10. What are TCP sequence numbers and their importance? **it allows the host to see if another host has successfully communicated back**
11. What is the significance if SYN/ACK/FIN in reference to TCP? **They are part of the TCP segment**
12. What happens if there is too much data to hold in a single packet? Does the network just get rid of that data? **No, it will usually time out**